

Attorney Docket No. 1448.1050

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:

Kiyoshi KOHIYAMA, et al.

Application No.:

Group Art Unit:

Filed: January 29, 2004

Examiner:

For: **METHOD OF AND APPARATUS FOR CREATING IMAGE PROCESSING PROGRAM,  
COMPUTER PROGRAM FOR CREATING IMAGE PROCESSING PROGRAM**

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN  
APPLICATION IN ACCORDANCE  
WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55**

Commissioner for Patents  
PO Box 1450  
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2003-063705

Filed: March 10, 2003

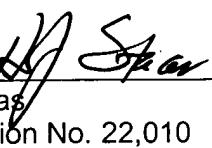
It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: January 29, 2004

By:

  
H. J. Staas  
Registration No. 22,010

1201 New York Ave, N.W., Suite 700  
Washington, D.C. 20005  
Telephone: (202) 434-1500  
Facsimile: (202) 434-1501

日本国特許庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2003年 3月10日  
Date of Application:

出願番号 特願2003-063705  
Application Number:

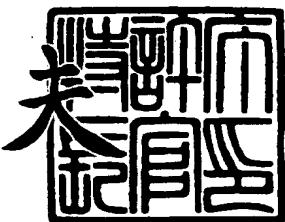
[ST. 10/C] : [JP 2003-063705]

出願人 富士通株式会社  
Applicant(s):

2003年11月26日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康



【書類名】 特許願  
【整理番号】 0340039  
【提出日】 平成15年 3月10日  
【あて先】 特許庁長官殿  
【国際特許分類】 H04N 7/08  
【発明の名称】 画像処理プログラム作成方法、画像処理プログラムの作成プログラムおよび画像処理プログラム作成装置  
【請求項の数】 10  
【発明者】  
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通  
株式会社内  
【氏名】 小桧山 清之  
【発明者】  
【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通  
株式会社内  
【氏名】 駒崎 弘  
【特許出願人】  
【識別番号】 000005223  
【氏名又は名称】 富士通株式会社  
【代理人】  
【識別番号】 100104190  
【弁理士】  
【氏名又は名称】 酒井 昭徳  
【手数料の表示】  
【予納台帳番号】 041759  
【納付金額】 21,000円  
【その他】 国等の委託研究の成果に係る特許出願（平成14年度通信・放送機構「PCなどオープンアーキテクチャーデジタル放送受信機に対応する権利保護システムの研究開発

」委託研究、産業活力再生特別措置法第30条の適用を  
受けるもの)

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9906241

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 画像処理プログラム作成方法、画像処理プログラムの作成プログラムおよび画像処理プログラム作成装置

【特許請求の範囲】

【請求項1】 暗号化および圧縮の少なくともいずれかがなされた動画像データに電子透かしデータを挿入する複数のプログラムの中から少なくとも一つをランダムに選択するプログラム選択工程と、

前記動画像データの復号および伸張の少なくともいずれかを行うプログラム内の複数の領域の中から前記プログラム選択工程で選択されたプログラムを挿入する領域として少なくとも一つをランダムに選択する領域選択工程と、

前記プログラム選択工程で選択されたプログラムを前記領域選択工程で選択された領域に挿入するプログラム挿入工程と、

を含んだことを特徴とする画像処理プログラム作成方法。

【請求項2】 前記電子透かしデータは、前記動画像データの復号および伸張の少なくともいずれかを行うプログラムを実行する画像処理装置に固有の情報を含むことを特徴とする前記請求項1に記載の画像処理プログラム作成方法。

【請求項3】 さらに、前記プログラム選択工程で選択されたプログラムの動作に必要なパラメータをランダムに決定するパラメータ決定工程を含み、

前記プログラム挿入工程では、前記パラメータ決定工程でパラメータを決定されたプログラムを前記領域選択工程で選択された領域に挿入することを特徴とする前記請求項1または請求項2に記載の画像処理プログラム作成方法。

【請求項4】 さらに、前記動画像データの復号および伸張の少なくともいずれかを行うプログラム内のジャンプ命令で指定された飛び先を前記プログラム挿入工程で挿入された複数のプログラムのうちいずれか一つから他の一つに書き換えるプログラム切り替え工程を含んだことを特徴とする前記請求項1～請求項3のいずれか一つに記載の画像処理プログラム作成方法。

【請求項5】 暗号化および圧縮の少なくともいずれかがなされた動画像データに電子透かしデータを挿入する複数のプログラムの中から少なくとも一つをランダムに選択させるプログラム選択工程と、

前記動画像データの復号および伸張の少なくともいずれかを行うプログラム内の複数の領域の中から前記プログラム選択工程で選択されたプログラムを挿入する領域として少なくとも一つをランダムに選択させる領域選択工程と、

前記プログラム選択工程で選択されたプログラムを前記領域選択工程で選択された領域に挿入させるプログラム挿入工程と、

をプロセッサに実行させることを特徴とする画像処理プログラムの作成プログラム。

**【請求項 6】** 前記電子透かしデータは、前記動画像データの復号および伸張の少なくともいずれかを行うプログラムを実行する画像処理装置に固有の情報を含むことを特徴とする前記請求項 5 に記載の画像処理プログラムの作成プログラム。

**【請求項 7】** さらに、前記プログラム選択工程で選択されたプログラムの動作に必要なパラメータをランダムに決定させるパラメータ決定工程を含み、

前記プログラム挿入工程では、前記パラメータ決定工程でパラメータを決定されたプログラムを前記領域選択工程で選択された領域に挿入させることを特徴とする前記請求項 5 または請求項 6 に記載の画像処理プログラムの作成プログラム。

**【請求項 8】** 暗号化および圧縮の少なくともいずれかがなされた動画像データに電子透かしデータを挿入する複数のプログラムの中から少なくとも一つをランダムに選択するプログラム選択手段と、

前記動画像データの復号および伸張の少なくともいずれかを行うプログラム内の複数の領域の中から前記プログラム選択手段により選択されたプログラムを挿入する領域として少なくとも一つをランダムに選択する領域選択手段と、

前記プログラム選択手段により選択されたプログラムを前記領域選択手段により選択された領域に挿入するプログラム挿入手段と、

を備えたことを特徴とする画像処理プログラム作成装置。

**【請求項 9】** 前記電子透かしデータは、前記動画像データの復号および伸張の少なくともいずれかを行うプログラムを実行する画像処理装置に固有の情報を含むことを特徴とする前記請求項 8 に記載の画像処理プログラム作成装置。

【請求項10】 さらに、前記プログラム選択手段により選択されたプログラムの動作に必要なパラメータをランダムに決定するパラメータ決定手段を備え、

前記プログラム挿入手段は、前記パラメータ決定手段によりパラメータを決定されたプログラムを前記領域選択手段により選択された領域に挿入することを特徴とする前記請求項8または請求項9に記載の画像処理プログラム作成装置。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

この発明は、動画像データを復号・伸張してモニターなどに出力するための画像処理プログラムを作成する画像処理プログラム作成方法、画像処理プログラムの作成プログラムおよび画像処理プログラム作成装置に関する。

##### 【0002】

##### 【従来の技術】

近年、情報のデジタル化技術の発達やインターネット（特にブロードバンドと呼ばれる高速なインターネット）の普及により、著作権法の保護を受ける各種の著作物がデジタル化され、CD-ROMやDVDといった各種メディア、インターネット・CATV・衛星放送といった各種伝送媒体を介して広く流通している。

##### 【0003】

これらデジタル化された情報に不可避的な問題として、正当な権利者に無断で行われる不正コピーの問題がある。つまり、デジタル化された情報は複製によつても劣化しないため、適法な範囲を超えて違法な複製が行われた場合（たとえば一時期流行した、インターネット上でのファイル交換など）は、当該情報についての著作権や使用権などを著しく侵害することになる。

##### 【0004】

この問題はすでに音楽の分野では顕著であり、音楽CDの売り上げが業界全体で落ち込むなど放置できない事態に発展しつつあるが、ここでは音楽に統いて、今後ますます深刻化することが予想される動画像（映画など）の不正コピー防止

について考える。

### 【0005】

図1は、従来技術による画像処理装置の構成を示す説明図である。インターネットなどで配信される動画像は、無権限者による伝送中の覗き見を防ぐため、所定の暗号鍵により暗号化されるとともに、データ量を抑制するため、MPEGなどの所定の方式で圧縮されている。そして、上記装置にはあらかじめ、上記動画像を復号・伸張するためのプログラム（以下では「画像処理プログラム」と呼ぶ）がインストールされている。

### 【0006】

NIC（ネットワーク・インターフェース・カード）100からPCIバス101を経由して、いったんHDD（ハードディスク）102に蓄積された上記動画像は、ユーザによる「視聴ボタン」の押下などを契機として、プロセッサ103によりメインメモリ104に読み出される。

### 【0007】

そして、同じくメインメモリ104に読み出された上記プログラムを実行するプロセッサ103が、上記動画像の復号および伸張を行い、次にグラフィックLSI105が、復号・伸張後の動画像を画像メモリ106に転送する。転送後の動画像は、グラフィックLSI105によりモニター107に表示できる形に変換され（たとえば、YPbPr形式からデジタルRGB信号に変換）、モニター107により表示される。

### 【0008】

上記装置においては、動画像の暗号復号鍵があらかじめ画像処理プログラムに組み込まれているため、解析によって当該鍵を抽出されてしまうおそれがある。また、復号（および伸張）後の動画像を、メインメモリ104や画像メモリ106から直接読み出されてしまう危険もある。パソコンなどのオープンアーキテクチャを採用する機器では、内部構造が広く一般に公開されているため、従来のAV機器などに比較して、上記のような行為の試みられる可能性が極めて高い。

### 【0009】

一方、画像メモリ106上のデータは動画像を含め、すべてプロセッサ103

から読み出すことができる。そのため動画像の再生中に、リアルタイムに画像メモリ106上のデータ（復号および伸張後の動画像）を読み出して、無断で複製したりインターネットで配信したりすることが可能である。

#### 【0010】

なお、こうした不正コピーが行われることを前提に、あるデータが違法に複製されたものであることを事後的に証明する技術として、いわゆる「電子透かし」がある（たとえば、特許文献1参照。）。

#### 【0011】

動画像は静止画像に比べると、全体としてかなり情報量が多く、しかもその大量の情報を短時間で処理しなければならない（たとえばNTSC（National Television System Committee）方式では、30分の1秒に1枚の画像を流さなければならない）。これは裏を返すと、個々の画像に電子透かしを入れるのにそれ以上の時間がかかるってはならないことを意味している。

#### 【0012】

こうした制約のもとで動画像に透かしを埋め込む技術はいくつか提案されているが、それらは大きく「見える透かし」と「見えない透かし」の2種類に分けられる。

#### 【0013】

##### （1）見える透かし

NHK-B/Sや一部のC/S放送に見られるような、画面の隅などに一定のロゴなどを表示し続ける方式である。透かしを入れる手順が簡単で入れるための時間も短く、しかも視聴者の誰にとっても透かしの存在が明瞭である。

#### 【0014】

##### （2）見えない透かし

正確には「見えない」のではなく、「人間の目には知覚されにくい」形で透かしを埋め込む方式である。元の画像を1次元あるいは2次元フーリエ変換により周波数成分に分解し、特定の高周波数成分（1つであっても複数であってもよい）に著作権者などのデータを挿入する。

#### 【0015】

## 【特許文献1】

特開平10-234012号公報

## 【0016】

## 【発明が解決しようとする課題】

しかしながら上記（1）の方式では、元の画像に余計なものが表示され続けるという不快感を視聴者に与えてしまう。また、透かしによってはそれほど難しくない手段で除去することが可能な場合もある。たとえば映画を放送する場合など、4:3のテレビ画面に映画のワイドスクリーン画像を入れるため、メインの画面の上下に黒帯ができるが、その部分に表示された透かしは除去が非常に簡単である。

## 【0017】

また、上記（2）の方式では電子透かしを挿入するアルゴリズムがいったん特定されてしまうと、挿入先の周波数成分を丸ごと削除することで、容易に透かしを除去できてしまう。これはもともと「見えづらい」部分の情報を削除するので、透かしを除去しても画質が大きく劣化することはない。

## 【0018】

そのため（2）の方式は、画質劣化の影響を極めて受け易い分野での応用が主体である。たとえば美術館の絵画などは、少しでも画質が劣化すれば価値が大幅に下がるため、インターネットでの公開などに際して透かしを挿入することは有効である。一方、動画像は元の画質もそれほど高くなく、透かしの除去による画質劣化で価値が極端に落ちるとも考えにくい。

## 【0019】

また、たとえ透かしを除去しないで複製したとしても、複製品中の透かしから分かるのは通常その著作権に関する情報（著作権者など）と、当該複製品が違法に複製された事実のみであり、違法に複製したのが誰であるかまでは分からず。インターネットを流れる情報は、一般にその配信元を特定するのが非常に困難であり、複製品が配信、再配信、再々配信されてしまうと、もともと誰がどのパソコンで無断で情報を複製・配信したのか特定するのは容易でない。

## 【0020】

複製元や配信元を特定できるようにするためには、複製時にパソコン上のソフトウェアで、電子透かしの中に当該パソコンの固有情報（製造番号など）を挿入するのが理想的であるが、上記ソフトウェアは容易に解析、改ざん、覗き見などができるので、アルゴリズムを解読されて上記機能を無効にされてしまう危険がある。

#### 【0021】

まとめると、従来技術により挿入された電子透かしは比較的除去が容易で、除去による画質劣化も少ないうえ、透かしからは違法な複製品の出所を確実に特定できないという問題があった。その結果、電子透かしを埋め込むことでは、不正コピーの抑止効果をほとんど期待できないという問題があった。

#### 【0022】

この発明は上記従来技術による問題を解決するため、パソコン内のメモリなどに存在する復号・伸張後の動画像の無断複製や無断配信を抑止することが可能な画像処理プログラム作成方法、画像処理プログラムの作成プログラムおよび画像処理プログラム作成装置を提供することを目的とする。

#### 【0023】

##### 【課題を解決するための手段】

上述した課題を解決し、目的を達成するため、この発明にかかる画像処理プログラム作成方法、画像処理プログラムの作成プログラムまたは画像処理プログラム作成装置は、暗号化および圧縮の少なくともいずれかがなされた動画像データに電子透かしデータを挿入する複数のプログラムの中から、少なくとも一つをランダムに選択するとともに、前記動画像データの復号および伸張の少なくともいずれかを行うプログラム内の複数の領域の中から、少なくとも一つをランダムに選択し、選択されたプログラムを選択された領域に挿入することを特徴とする。

#### 【0024】

また、この発明にかかる画像処理プログラム作成方法、画像処理プログラムの作成プログラムまたは画像処理プログラム作成装置は、前記電子透かしデータが、前記動画像データの復号および伸張の少なくともいずれかを行うプログラムを実行する画像処理装置に固有の情報を含むことを特徴とする。

**【0025】**

また、この発明にかかる画像処理プログラム作成方法、画像処理プログラムの作成プログラムまたは画像処理プログラム作成装置は、さらに、上記で選択されたプログラムの動作に必要なパラメータをランダムに決定するとともに、パラメータを決定されたプログラムを上記で選択された領域に挿入することを特徴とする。

**【0026】**

また、この発明にかかる画像処理プログラム作成方法は、さらに、前記動画像データの復号および伸張の少なくともいずれかを行うプログラム内のジャンプ命令で指定された飛び先を上記で挿入された複数のプログラムのうちいずれか一つから他の一つに書き換えることを特徴とする。

**【0027】**

これらの発明により作成されたプログラムは、動画像の再生時（厳密には復号・伸張時）に、その再生元を特定できるような情報をランダムに、すなわち、規則性がないためにその除去が極めて困難な態様で当該動画像に埋め込むので、複製品に承継された上記情報から、その無断複製者を迅速かつ確実に特定することができる。

**【0028】****【発明の実施の形態】**

以下に添付図面を参照して、この発明にかかる画像処理プログラム作成方法、画像処理プログラムの作成プログラムおよび画像処理プログラム作成装置の好適な実施の形態を詳細に説明する。

**【0029】****(実施の形態1)**

図2は、本発明の実施の形態1による画像処理装置の構成を示す説明図である。図2において、NIC（ネットワーク・インターフェース・カード）200からPCIバス201を経由して、いったんHDD（ハードディスク）202に蓄積された上記動画像は、ユーザによる「視聴ボタン」の押下などを契機として、プロセッサ203によりメインメモリ204に読み出される。

## 【0030】

そして、同じくメインメモリ204に読み出された上記プログラムを実行するプロセッサ203が、上記動画像の復号および伸張を行い、次にグラフィックLSI205が、復号・伸張後の動画像を画像メモリ206に転送する。転送後の動画像は、グラフィックLSI205によりモニター207に表示できる形に変換され（たとえば、YPbPr形式からデジタルRGB信号に変換）、モニター207により表示される。

## 【0031】

図2において、図1に示した従来技術の構成と比較すると、ハードウェアとしては、TRM (Tamper Resistant Module) 208が新たに追加されている。このTRM208とは、外部から覗き見、改ざん、解析しようとすると内部が破壊されるよう設計されたハードウェアであり、たとえばPCカードなどに埋め込まれて、PCカードスロットを介してパソコンと接続される。なお、このTRM208が本発明にいう画像処理プログラム作成装置に相当する。

## 【0032】

また、ソフトウェア的にはn種類の電子透かし挿入モジュール群、および個々のモジュールの暗号復号鍵群が追加されている。本装置において画像処理プログラムを構成する暗号復号モジュール・MPEG伸張モジュール・電子透かし挿入モジュール（およびその暗号復号鍵群）は、いずれも暗号化された形でHDD202内に散在している。

## 【0033】

また、図3は本発明の実施の形態1による画像処理プログラム作成装置（具体的にはTRM208）のハードウェア構成を示す説明図である。208aはPCIバスインターフェースであり、PCIバス201とのデータの授受を制御する。208bはプロセッサであり、TRM208全体の動作を制御する。208cはプロセッサメモリであり、プロセッサ208b用のプログラムやワークエリアを提供する。

## 【0034】

208dは動画像用の暗号復号鍵、暗号復号モジュール、MPEG伸張モジュ

ール、および電子透かし挿入モジュール用の暗号復号鍵を復号するための暗号復号マスター鍵である。208eは暗号復号マスター鍵208dを用いて、入力データの復号を行う暗号復号回路である。また、208fは現在日時を計測するタイマ、208gは後述する電子署名を作成するための暗号化鍵、208hは暗号化鍵208gを用いて入力データの暗号化を行う暗号化回路（ハッシュ回路）である。

### 【0035】

次に、図4は本発明の実施の形態1による画像処理プログラム作成装置（具体的にはTRM208）における、画像処理プログラムの作成処理の手順を示すフローチャートである。

### 【0036】

図示する処理の開始に先立って、HDD202には動画像、および当該動画像を復号するための暗号復号鍵（動画像とともに配布）が保存されているものとする。そして、ユーザが上記動画像を指定してその視聴を指示すると、当該指示がPCIバス201およびPCIバスインターフェース208aを介してTRM208に伝達され、TRM208のプロセッサ208bが、プロセッサメモリ208cに保持されたプログラム（画像処理プログラムの作成プログラム）に従って以下の処理を実行する。

### 【0037】

プロセッサ208bは、まず上記動画像を復号するための暗号復号鍵を、HDD202からPCIバス201・PCIバスインターフェース208aを介してプロセッサメモリ208cに読み出す（ステップS401）。そして、当該鍵と当該鍵を復号するための暗号復号マスター鍵208dとを、暗号復号回路208eに供給することで、ステップS401で読み出した暗号復号鍵の復号を行う（ステップS402）。

### 【0038】

次に、プロセッサ208bは上記動画像に電子透かしとして埋め込むデータを作成する（ステップS403）。このデータとは、具体的には

- (1) TRM208ごとに割り振られた固有番号であるTRM番号（平文）

(2) 現在日時（平文）

(3) TRM208の暗号化鍵208gで暗号化されたTRM番号+現在日時を合わせたものである。

#### 【0039】

このうち（3）は、上記暗号化鍵208gがなければ作成できない（暗号化後のデータを解析して逆に暗号化鍵208gを特定することは、数学的に極めて困難であることが証明されている）ことから、逆にその作成元が当該鍵を有するTRM208であることを保障できる。言い換えれば、本発明では動画像の視聴時に、TRM208の電子署名を電子透かしとして挿入することになる。なお、上記動画像にすでに著作権情報などの透かしが入っている場合は、本発明により重ねて透かしが入れられることになる。

#### 【0040】

プロセッサ208bは暗号化回路208hに、プロセッサメモリ208cから読み出したTRM番号、タイマ208fから読み出した現在日時、およびハッシュに必要な暗号化鍵208gを供給する。そして、暗号化前のTRM番号と現在日時とを、暗号化後のTRM番号および現在日時と組み合わせて透かしデータを作成する（ステップS403）。なお、TRM番号や現在日時以外の情報を適宜透かしデータに加えてもよい。

#### 【0041】

次に、プロセッサ208bはHDD202に保持されたn種類の電子透かし挿入モジュールの中から、いずれか一つをランダムに選択する（ステップS404）とともに、選択したモジュールと当該モジュール用の暗号復号鍵とを、HDD202からPCIバス201・PCIバスインターフェース208aを介してプロセッサメモリ208cに読み出す（ステップS405）。

#### 【0042】

個々の電子透かし挿入モジュールは、それぞれ対応する暗号復号鍵により暗号化されており、この暗号復号鍵もまた暗号化されている。プロセッサ208bは、暗号復号マスター鍵208dおよび暗号復号回路208eにより上記で読み出した暗号復号鍵を復号する（ステップS406）とともに、復号後の暗号復号鍵

により上記で読み出した電子透かし挿入モジュールを復号する（ステップS407）。

#### 【0043】

次に、プロセッサ208bは復号後の上記モジュールが必要とするパラメータをランダムに決定のうえ、ステップS403で作成した透かしデータとともにモジュール内に設定する（ステップS408）。

#### 【0044】

このパラメータとは、たとえば選択したモジュールが上述の「見える透かし」を挿入する場合は、透かしを挿入する位置（場所）や大きさなど、「見えない透かし」を挿入する場合は透かしを挿入する周波数帯などである。また、いずれの方式にも共通するパラメータとして、挿入間隔すなわち連続する動画像のうちどの画像に透かしを入れるか（1枚ごと、10枚ごと、乱数によりランダムに発生した枚数ごと、など）がある。

#### 【0045】

次に、プロセッサ208bはHDD202に保持された暗号復号モジュールおよびMPEG伸張モジュールを、PCIバス201・PCIバスインターフェース208aを介してプロセッサメモリ208cに読み出す（ステップS409）。これらのモジュールも暗号化されているので、プロセッサ208bは暗号復号マスター鍵208dおよび暗号復号回路208eによりその復号を行う（ステップS410）。

#### 【0046】

さらにプロセッサ208bは、ステップS402で復号した、動画像を復号するための暗号復号鍵を、ステップS410で復号した暗号復号モジュールに埋め込む（ステップS411）。

#### 【0047】

また、復号後のMPEG伸張モジュールには、あらかじめ決められた位置にNOP領域（命令やデータのない空き領域）が設けられている。プロセッサ208bは、複数のNOP領域の中からいずれか一つをランダムに選択し、当該領域にパラメータ設定後の電子透かし挿入モジュールを埋め込む（ステップS412）

。

### 【0048】

次に、プロセッサ208bは暗号復号鍵埋め込み後の暗号復号モジュールと、電子透かし挿入モジュール埋め込み後のMPEG伸張モジュールとを結合することで、画像処理プログラムを完成させる（ステップS413）。そして、完成した上記プログラムをPCIバスインターフェース208aおよびPCIバス201を介して、メインメモリ204に出力する（ステップS414）。

### 【0049】

この後制御はプロセッサ203に移り、プロセッサ203はメインメモリ204にロードされた上記プログラムを実行することで、視聴が指示された動画像をモニター207に出力する。図5は、本発明の実施の形態1による画像処理装置における、動画像の再生処理の手順を示すフローチャートである。

### 【0050】

まず、HDD202上の動画像をメインメモリ204に読み出すとともに（ステップS501）、上述の暗号復号モジュールにより当該動画像を復号する（ステップS502）。なお、復号に必要な暗号復号鍵（動画像とともに暗号化されて配布）は、上述のようにすでに暗号復号マスター鍵208dにより復号され、上記モジュール内に組み込まれている。復号後の動画像、すなわち圧縮MPEG動画像は、いったんメインメモリ204に蓄積される。

### 【0051】

次に、プロセッサ203は圧縮MPEG動画像をメインメモリ204から読み出し、上述のMPEG伸張モジュールによりその伸張を行う（ステップS503）。なお、伸張された動画像は一般にYCbCr形式である。

### 【0052】

そして、このYCbCr画像に、MPEG伸張モジュールのNOP領域に組み込まれた上述の電子透かし挿入モジュールが、TRM番号などからなる透かしデータを埋め込む（ステップS504）。透かしデータの挿入位置や周波数帯などは、モジュール内に設定されたパラメータに従う。なお、すべての画像でなく、何枚ごとというように間欠的に透かしを入れる設定がされている場合は、条件に

該当する画像のみに透かしを挿入する。

#### 【0053】

電子透かし挿入後のY Pb Pr画像は、再びメインメモリ204に一時保存され、次にグラフィックLSI205が、上記画像を画像メモリ206に転送する（ステップS505）。そして、このY Pb Pr画像をたとえばデジタルRGB信号に変換し（ステップS506）、モニター207に出力・表示する（ステップS507）。

#### 【0054】

以上説明した実施の形態1によれば、画像メモリ206上のY Pb Pr画像を横取り（ハッキング）してインターネットに流しても、その画像の中にはTRM208の固有番号と再生日時、すなわち、いつ誰がどのパソコン（厳密には、どのTRM208）でコンテンツを再生したかが電子透かしとして埋め込まれている。コンテンツの販売元がもともと埋め込んでいる著作権情報などに加えて、販売後の視聴時に、ユーザのパソコンでさらにTRM番号などが挿入されることによって、正当な権利者は自己の著作物が違法に複製されたことを証明できるとともに、複製品の出所を確実に特定することができる。

#### 【0055】

なお、電子透かしを実際に挿入するのはTRM208側のプロセッサ208bでなく、パソコン本体側のプロセッサ203なので（プロセッサ208bは電子透かし挿入モジュールを選択・復号して、メインメモリ204に出力するのみである）、TRM208に搭載されたプロセッサ208bの性能が低くても、複雑かつ高度なアルゴリズムによる透かしの埋め込みが可能である。

#### 【0056】

##### （実施の形態2）

さて、上述した実施の形態1では、MPEG伸張モジュールに組み込まれる電子透かし挿入モジュールが「毎回」（再生の都度、の意）異なるので、仮にある映像作品Aについて透かしを除去できても、別の映像作品Bの透かしを除去するには改めて解析を行わなければならない。しかも、上記モジュールのプログラム内での位置（MPEG伸張モジュール内のどこに組み込まれるか）も毎回変化す

るので、透かしを埋め込んでいるのがプログラムのどの部分であるかさえ特定困難である。

### 【0057】

ただ、実施の形態1ではAについて透かしのアルゴリズムを特定されてしまつたために、それ以外のB・C・D・・・の透かしが連鎖的に除去されることは回避できるものの、Aについては透かしの除去や、除去後の無断複製・無断配信を阻止することができない。そこで、以下に説明する実施の形態2のように、そもそも一つの動画像についても透かしの除去が不可能（原理上は可能であるが、事实上は不可能）となるようにしてもよい。

### 【0058】

本発明の実施の形態2による画像処理装置の構成は、図2に示した実施の形態1のそれと同一である（TRM208の構成も、図3に示した実施の形態1のそれと同一である）。異なるのは、TRM208のプロセッサメモリ208cに、図4に示した処理を実行するプログラム以外に、ステップS414でメインメモリ204に出力された後のプログラムを書き換えるためのプログラムが保持されている点である。

### 【0059】

また、実施の形態2によるプロセッサ208bは、図4のステップS404において電子透かし挿入モジュールを複数選択する。これに伴って、ステップS408では選択された各モジュールにつきパラメータが決定・設定され、ステップS412ではそれぞれのモジュールにつき挿入先のNOP領域が選択される。

### 【0060】

図6は、本発明の実施の形態2による画像処理プログラム作成装置（具体的にはTRM208）で作成される、画像処理プログラムの内部構造を模式的に示す説明図である。図中「XXXX」と記された部分は、暗号復号モジュールあるいはMPEG伸張モジュールのコードである。「AAAA」および「BBBB」と記された部分が、それぞれ別個の電子透かし挿入モジュールである。なお、「AAAA」「BBBB」の末尾がいずれもリターン命令であることから、電子透かし挿入モジュールはいずれもサブルーティンであることが分かる。

### 【0061】

図6に示した画像処理プログラムは、TRM208による作成後、メインメモリ204の特定のメモリ領域にロードされて、プロセッサ203により実行される。プロセッサ203は図示するプログラムを逐次実行し、ジャンプ命令600に出合うと、指定された飛び先、すなわち図示する例ではNOP1にジャンプして、電子透かし挿入モジュール1の手順により透かしを挿入する。

### 【0062】

ここで、上記プログラムの実行中に、ジャンプ命令600の飛び先を「NOP1」から「NOP2」に書き換えてやれば、以後上記プログラムはモジュール2の手順により透かしを埋め込むことになる。このように、実際に使用する電子透かし挿入モジュールをリアルタイムに変更することで、一連の動画像を構成する個々の画像について、それぞれ異なるアルゴリズムにより透かしを挿入することができる。

### 【0063】

図7は、本発明の実施の形態2による画像処理プログラム作成装置（具体的にはTRM208）における、電子透かし挿入モジュール切り替え処理の手順を示すフローチャートである。

### 【0064】

図示する処理の開始に先立って、TRM208のプロセッサメモリ208cには、図4のステップS412でプロセッサ208bがどの電子透かし挿入モジュールを、MPEG伸張モジュール内のどのNOP領域にはめ込んだかの対照表が作成・保存されているものとする。また、図示する処理はプロセッサ203で画像処理プログラムが実行されている間、プロセッサ208bにより繰り返し実行される。

### 【0065】

TRM208のプロセッサ208bは、まず、電子透かし挿入モジュールの切り替えまでの待ち時間を乱数などによりランダムに決定する（ステップS701）。そして上記で決定した待ち時間が経過すると（ステップS702：Yes）、上記の対照表を参照して、いずれか一つの電子透かし挿入モジュールをランダ

ムに選択するとともに（ステップS703）、選択したモジュールの位置すなわち当該モジュールがMPEG伸張モジュールのどのNOP領域に組み込まれているかを読み出す（ステップS704）。

#### 【0066】

その後、メインメモリ204への書き込み命令に、書き込み先のアドレス（具体的には、上述のジャンプ命令600が格納されているアドレス）とジャンプ命令600の新たな飛び先（ここでは「NOP2」の開始アドレス）を添えて、PCIバスインターフェース208aからPCIバス201に送出する（ステップS705）。そして、これを受けたプロセッサ203が、上記命令に従ってメインメモリ204上のジャンプ命令600を書き換える（ステップS706）。

#### 【0067】

なお、ここではあらかじめ複数の電子透かし挿入モジュールをメインメモリ204にロードしておき、ジャンプ命令600の飛び先を変更することで実際に使用するモジュールを切り替えたが、逆にその飛び先にあるモジュールをプロセッサ208bから書き換える（実際に使用するモジュールをその都度メインメモリ204にロードする）ことで、透かしの挿入アルゴリズムを変更することもできる。たとえば図6の例であれば、ジャンプ命令600の飛び先は常にNOP1のまま、NOP1内のコードを「AAAA」から「BBBB」に差し替える。

#### 【0068】

以上説明した実施の形態2によれば、一つの動画像の中でも、個々の画像ごとに透かしの挿入アルゴリズムが異なるので、たとえある種の透かしの除去に成功したとしても、動画像を構成するすべての画像から透かしを除去することは事实上不可能である。

#### 【0069】

そのため、ハッカーは画像メモリ204からハックしたコンテンツを、電子透かしが埋め込まれたままで複製することになる。コンテンツの提供元であるサービスプロバイダーは、インターネットなどで自己のコンテンツの違法な複製品が多数流通していることを検知すると、その出所を特定するために、複製品とおぼしきコンテンツの解析を専門の電子透かし解析業者に委託する。

## 【0070】

従来技術と異なり、本発明により埋め込まれる電子透かしは動画像ごと、あるいは一連の動画像を構成する画像ごとにランダムに変化するので、複製品の中から電子透かしを抽出するのは従来と比べ格段に困難である。もっとも、ハッカーがTRM番号、すなわち複製品の出所を分からなくするために動画像内のすべての透かしを除去しなければならないのに対して、解析業者が出所を特定するには、動画像中の一枚でも透かしの抽出に成功すればよい。

## 【0071】

上述のように、電子透かしには暗号化されたTRM番号が含まれ、この暗号化はサービスプロバイダーなど、一部の人間しか知らない暗号化鍵208gがなければ不可能なので、逆に上記電子透かしが、当該暗号化鍵208gを保持するTRM208により挿入されたことの有力な証拠となる。すなわち、その電子透かし入りの複製品が上記TRM208の組み込まれたパソコンからハックされたことはほぼ確実なので、その所有者などを警察に通報し、法的に処罰すればよい（図8）。

## 【0072】

なお、上述した実施の形態1および2は動画像への電子透かしの挿入を例として説明したが、たとえば静止画、音声／音楽、テキストなどについても、表示／再生元を特定できるような情報を透かしとして埋め込んだり、埋め込みのアルゴリズムをその都度変更したりすることは、不正コピーの抑止の観点から非常に有効である。

## 【0073】

なお、図4や図7に示した処理を実行するプログラムは、TRM208のほかたとえばフレキシブルディスク、ROM、CD-ROM、CD-RW、MO、DVDなどプロセッサで読み取り可能な各種の記録媒体に記録され、当該記録媒体によって配布することができる。また、インターネットなどのネットワークを介して配布することも可能である。

## 【0074】

（付記1）暗号化および圧縮の少なくともいずれかがなされた動画像データに電

子透かしデータを挿入する複数のプログラムの中から少なくとも一つをランダムに選択するプログラム選択工程と、

前記動画像データの復号および伸張の少なくともいずれかを行うプログラム内の複数の領域の中から前記プログラム選択工程で選択されたプログラムを挿入する領域として少なくとも一つをランダムに選択する領域選択工程と、

前記プログラム選択工程で選択されたプログラムを前記領域選択工程で選択された領域に挿入するプログラム挿入工程と、

を含んだことを特徴とする画像処理プログラム作成方法。

#### 【0075】

(付記2) 前記電子透かしデータは、前記動画像データの復号および伸張の少なくともいずれかを行うプログラムを実行する画像処理装置に固有の情報を含むことを特徴とする前記付記1に記載の画像処理プログラム作成方法。

#### 【0076】

(付記3) 前記電子透かしデータは、前記動画像データの復号および伸張の少なくともいずれかを行うプログラムを実行する画像処理装置を構成するTRMの固有番号および当該TRMに固有の暗号化鍵により暗号化された前記固有番号を含むことを特徴とする前記付記1に記載の画像処理プログラム作成方法。

#### 【0077】

(付記4) さらに、前記プログラム選択工程で選択されたプログラムの動作に必要なパラメータをランダムに決定するパラメータ決定工程を含み、

前記プログラム挿入工程では、前記パラメータ決定工程でパラメータを決定されたプログラムを前記領域選択工程で選択された領域に挿入することを特徴とする前記付記1～付記3のいずれか一つに記載の画像処理プログラム作成方法。

#### 【0078】

(付記5) さらに、前記動画像データの復号および伸張の少なくともいずれかを行うプログラム内のジャンプ命令で指定された飛び先を前記プログラム挿入工程で挿入された複数のプログラムのうちいずれか一つから他の一つに書き換えるプログラム切り替え工程を含んだことを特徴とする前記付記1～付記4のいずれか一つに記載の画像処理プログラム作成方法。

## 【0079】

(付記6) 前記プログラム切り替え工程では、前記動画像データの復号および伸張の少なくともいずれかを行うプログラムの実行中に前記飛び先を書き換えることを特徴とする前記付記5に記載の画像処理プログラム作成方法。

## 【0080】

(付記7) 暗号化および圧縮の少なくともいずれかがなされた動画像データに電子透かしデータを挿入する複数のプログラムの中から少なくとも一つをランダムに選択させるプログラム選択工程と、

前記動画像データの復号および伸張の少なくともいずれかを行うプログラム内の複数の領域の中から前記プログラム選択工程で選択されたプログラムを挿入する領域として少なくとも一つをランダムに選択させる領域選択工程と、

前記プログラム選択工程で選択されたプログラムを前記領域選択工程で選択された領域に挿入させるプログラム挿入工程と、

をプロセッサに実行させることを特徴とする画像処理プログラムの作成プログラム。

## 【0081】

(付記8) 前記電子透かしデータは、前記動画像データの復号および伸張の少なくともいずれかを行うプログラムを実行する画像処理装置に固有の情報を含むことを特徴とする前記付記7に記載の画像処理プログラムの作成プログラム。

## 【0082】

(付記9) 前記電子透かしデータは、前記動画像データの復号および伸張の少なくともいずれかを行うプログラムを実行する画像処理装置を構成するTRMの固有番号および当該TRMに固有の暗号化鍵により暗号化された前記固有番号を含むことを特徴とする前記付記7に記載の画像処理プログラムの作成プログラム。

## 【0083】

(付記10) さらに、前記プログラム選択工程で選択されたプログラムの動作に必要なパラメータをランダムに決定させるパラメータ決定工程を含み、

前記プログラム挿入工程では、前記パラメータ決定工程でパラメータを決定されたプログラムを前記領域選択工程で選択された領域に挿入させることを特徴と

する前記付記7～付記9のいずれか一つに記載の画像処理プログラムの作成プログラム。

#### 【0084】

(付記11) さらに、前記動画像データの復号および伸張の少なくともいずれかを行うプログラム内のジャンプ命令で指定された飛び先を前記プログラム挿入工程で挿入された複数のプログラムのうちいずれか一つから他の一つに書き換えさせるプログラム切り替え工程をプロセッサに実行させることを特徴とする前記付記7～付記10のいずれか一つに記載の画像処理プログラムの作成プログラム。

#### 【0085】

(付記12) 前記プログラム切り替え工程では、前記動画像データの復号および伸張の少なくともいずれかを行うプログラムの実行中に前記飛び先を書き換えさせることを特徴とする前記付記11に記載の画像処理プログラムの作成プログラム。

#### 【0086】

(付記13) 暗号化および圧縮の少なくともいずれかがなされた動画像データに電子透かしデータを挿入する複数のプログラムの中から少なくとも一つをランダムに選択するプログラム選択手段と、

前記動画像データの復号および伸張の少なくともいずれかを行うプログラム内の複数の領域の中から前記プログラム選択手段により選択されたプログラムを挿入する領域として少なくとも一つをランダムに選択する領域選択手段と、

前記プログラム選択手段により選択されたプログラムを前記領域選択手段により選択された領域に挿入するプログラム挿入手段と、

を備えたことを特徴とする画像処理プログラム作成装置。

#### 【0087】

(付記14) 前記電子透かしデータは、前記動画像データの復号および伸張の少なくともいずれかを行うプログラムを実行する画像処理装置に固有の情報を含むことを特徴とする前記付記13に記載の画像処理プログラム作成装置。

#### 【0088】

(付記15) 前記電子透かしデータは、前記動画像データの復号および伸張の少

なくともいずれかを行うプログラムを実行する画像処理装置を構成するTRMの固有番号および当該TRMに固有の暗号化鍵により暗号化された前記固有番号を含むことを特徴とする前記付記13に記載の画像処理プログラム作成装置。

#### 【0089】

(付記16) さらに、前記プログラム選択手段により選択されたプログラムの動作に必要なパラメータをランダムに決定するパラメータ決定手段を備え、

前記プログラム挿入手段は、前記パラメータ決定手段によりパラメータを決定されたプログラムを前記領域選択手段により選択された領域に挿入することを特徴とする前記付記13～付記15のいずれか一つに記載の画像処理プログラム作成装置。

#### 【0090】

(付記17) さらに、前記動画像データの復号および伸張の少なくともいずれかを行うプログラム内のジャンプ命令で指定された飛び先を前記プログラム挿入手段により挿入された複数のプログラムのうちいずれか一つから他の一つに書き換えるプログラム切り替え手段を備えたことを特徴とする前記付記13～付記16のいずれか一つに記載の画像処理プログラム作成装置。

#### 【0091】

(付記18) 前記プログラム切り替え手段は、前記動画像データの復号および伸張の少なくともいずれかを行うプログラムの実行中に前記飛び先を書き換えることを特徴とする前記付記17に記載の画像処理プログラム作成装置。

#### 【0092】

##### 【発明の効果】

以上説明したように本発明により作成されたプログラムは、動画像の再生時（厳密には復号・伸張時）に、その再生元を特定できるような情報をランダムに、すなわち、規則性がないためにその除去が極めて困難な態様で当該動画像に埋め込むので、複製品に承継された上記情報から、その無断複製者を迅速かつ確実に特定することができ、これによって、パソコン内のメモリなどに存在する復号・伸張後の動画像の無断複製や無断配信を抑止することが可能な画像処理プログラム作成方法、画像処理プログラムの作成プログラムおよび画像処理プログラム作

成装置が得られるという効果を奏する。

【図面の簡単な説明】

【図1】

従来技術による画像処理装置の構成を示す説明図である。

【図2】

本発明の実施の形態1による画像処理装置の構成を示す説明図である。

【図3】

本発明の実施の形態1による画像処理プログラム作成装置（具体的にはTRM208）のハードウェア構成を示す説明図である。

【図4】

本発明の実施の形態1による画像処理プログラム作成装置（具体的にはTRM208）における、画像処理プログラムの作成処理の手順を示すフローチャートである。

【図5】

本発明の実施の形態1による画像処理装置における、動画像の再生処理の手順を示すフローチャートである。

【図6】

本発明の実施の形態2による画像処理プログラム作成装置（具体的にはTRM208）で作成される、画像処理プログラムの内部構造を模式的に示す説明図である。

【図7】

本発明の実施の形態2による画像処理プログラム作成装置（具体的にはTRM208）における、電子透かし挿入モジュール切り替え処理の手順を示すフローチャートである。

【図8】

コンテンツが販売されてから違法な複製品の出所が特定されるまでの流れを模式的に示す説明図である。

【符号の説明】

100, 200 N I C

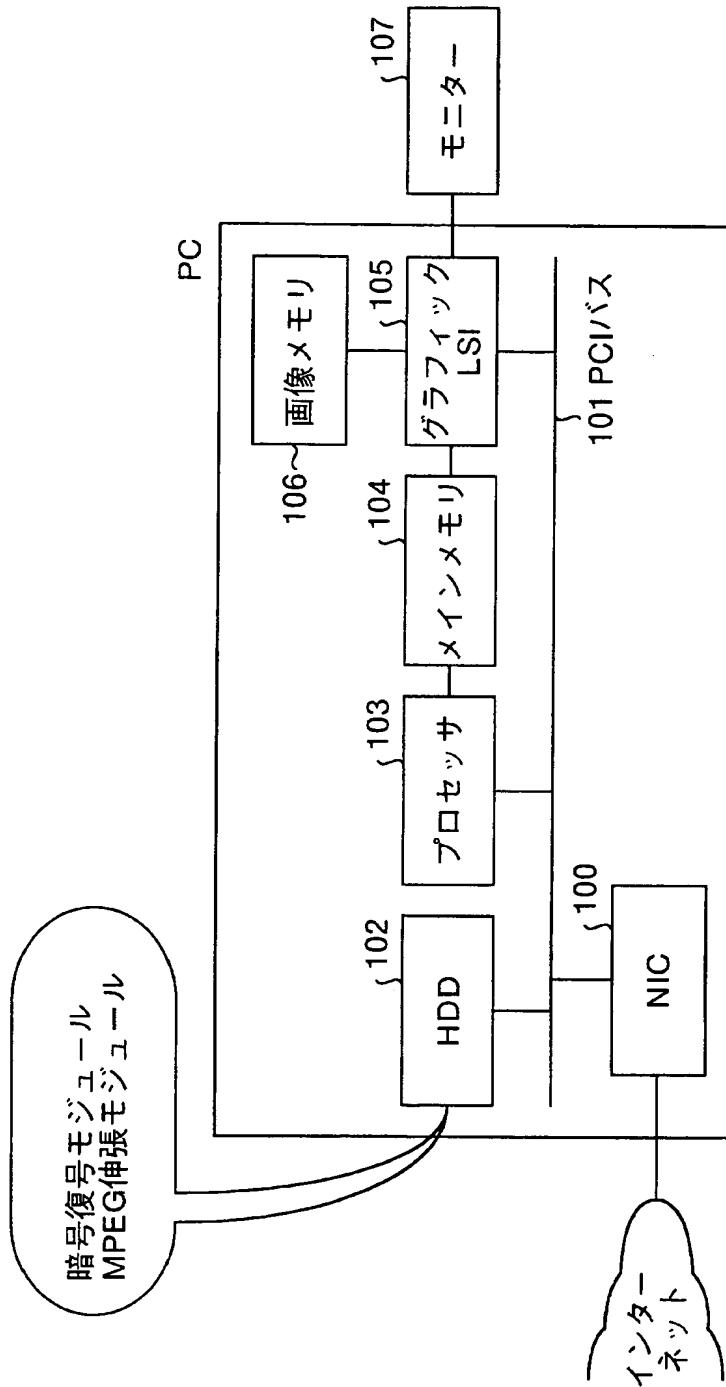
101, 201 PCIバス  
102, 202 HDD  
103, 203 プロセッサ  
104, 204 メインメモリ  
105, 205 グラフィックLSI  
106, 206 画像メモリ  
107, 207 モニター  
208 TRM  
208a PCIバスインターフェース  
208b プロセッサ  
208c プロセッサメモリ  
208d 暗号復号マスター鍵  
208e 暗号復号回路  
208f タイマ  
208g 暗号化鍵  
208h 暗号化回路

【書類名】

図面

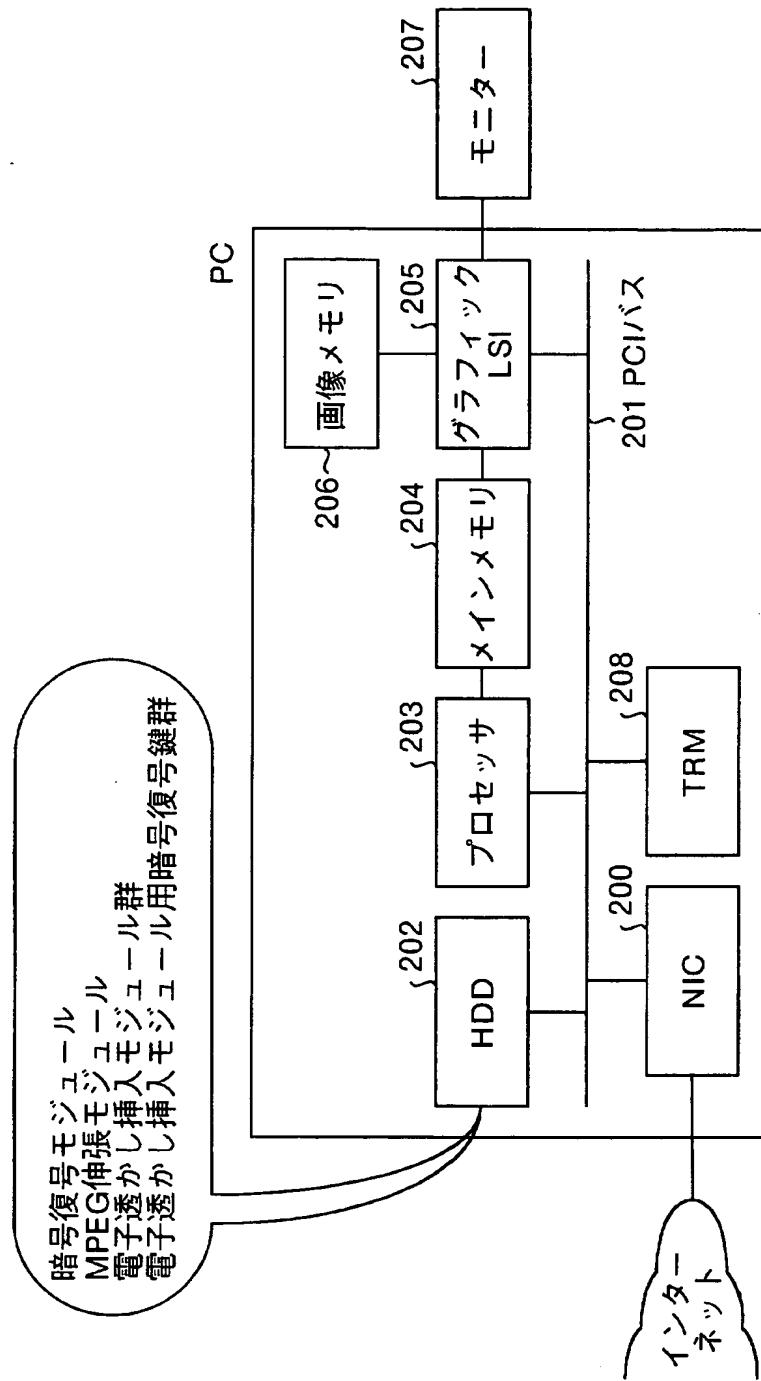
【図 1】

従来技術による画像処理装置の構成を示す説明図



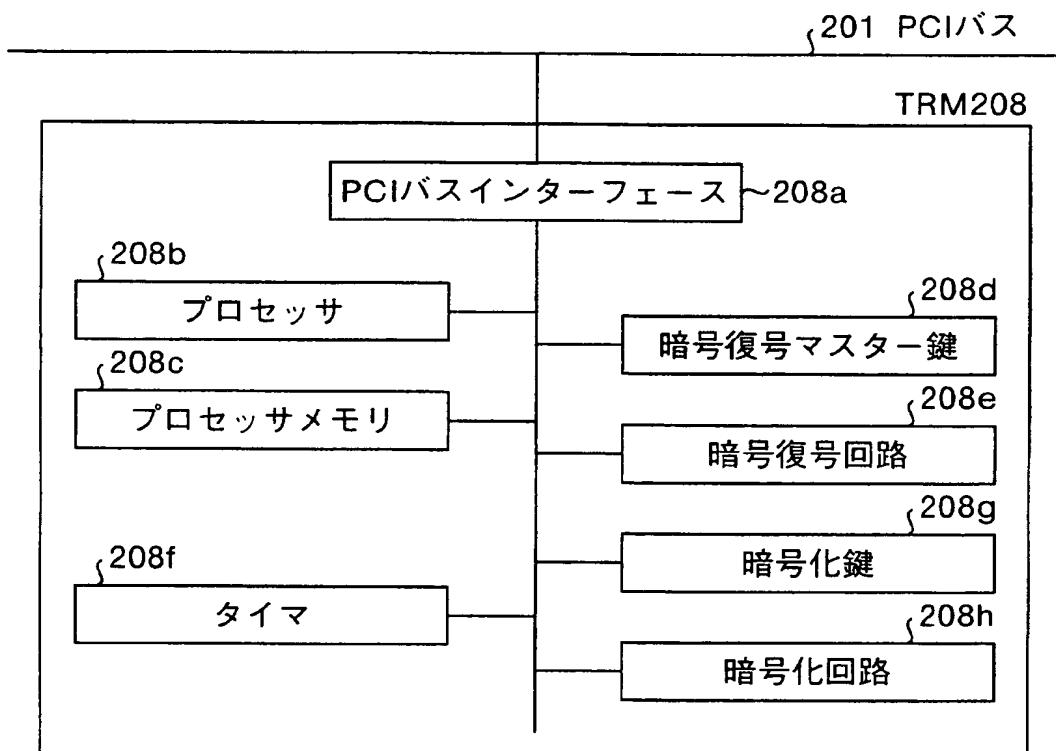
【図 2】

本発明の実施の形態1による画像処理装置の構成を示す説明図



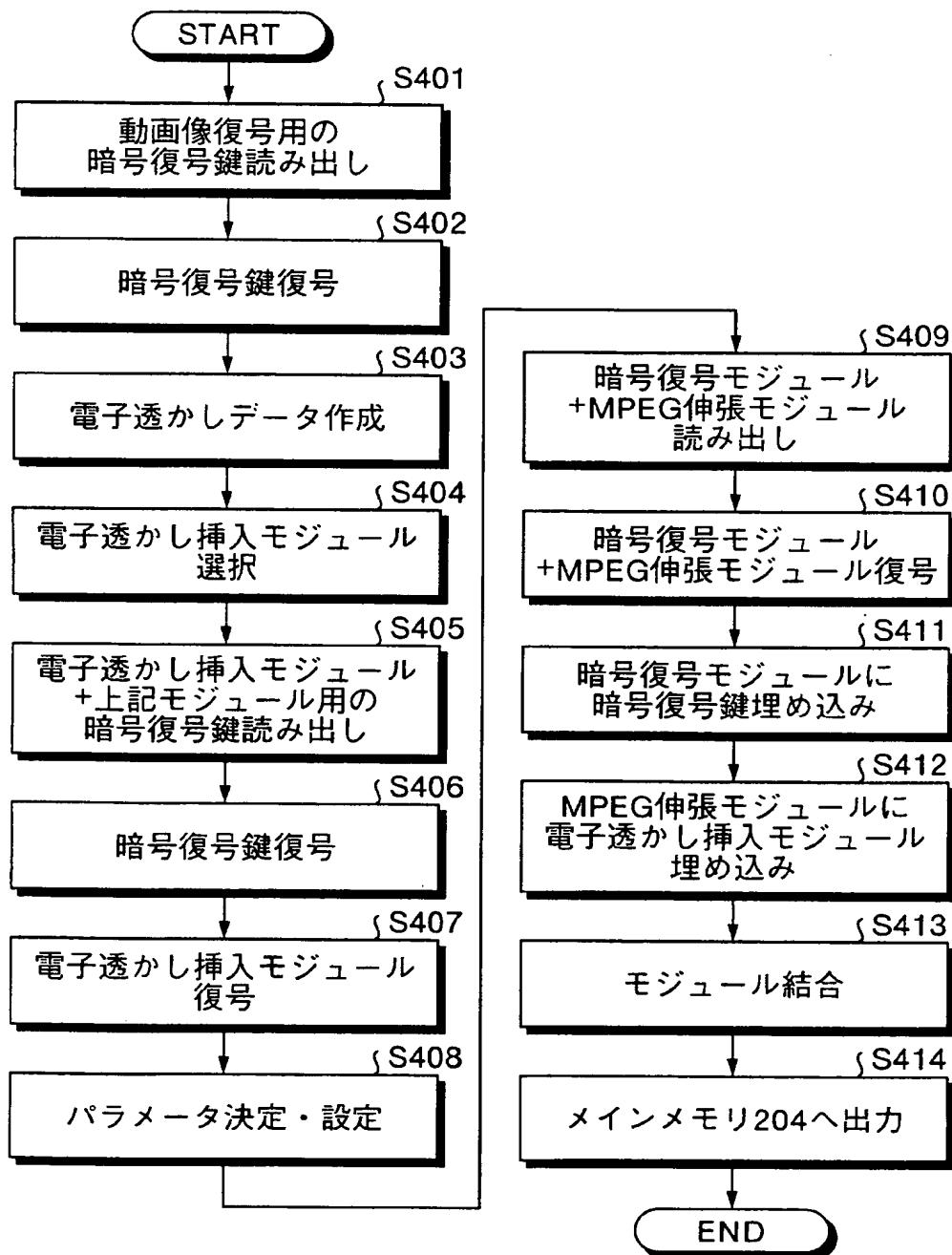
【図3】

本発明の実施の形態1による画像処理プログラム作成装置  
(具体的にはTRM208) のハードウェア構成を示す説明図



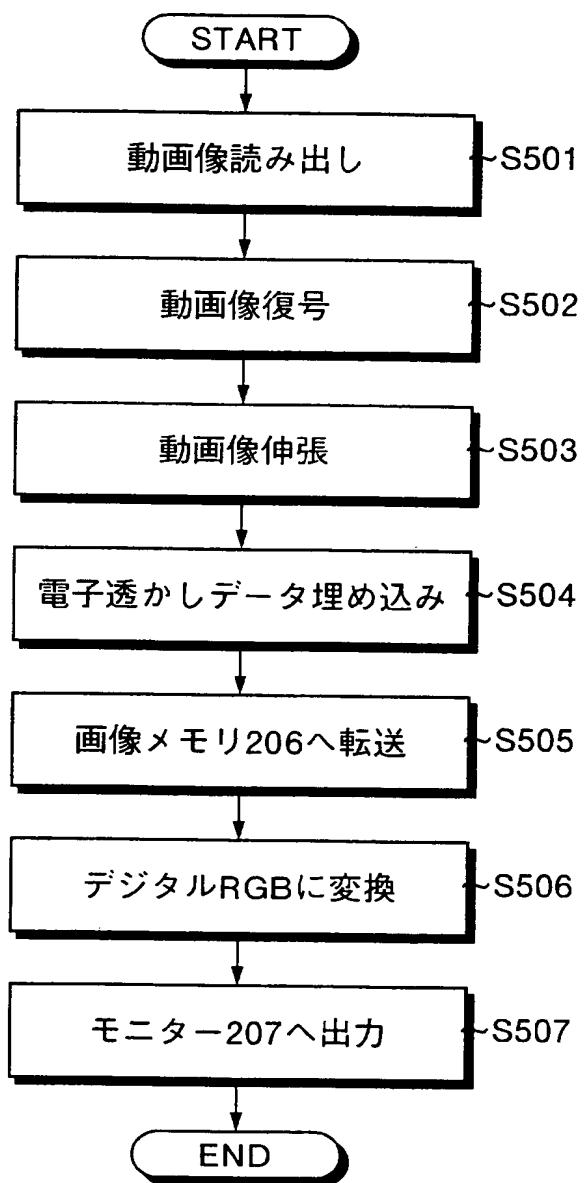
【図4】

本発明の実施の形態1による画像処理プログラム作成装置  
(具体的にはTRM208) における、画像処理プログラムの  
作成処理の手順を示すフローチャート



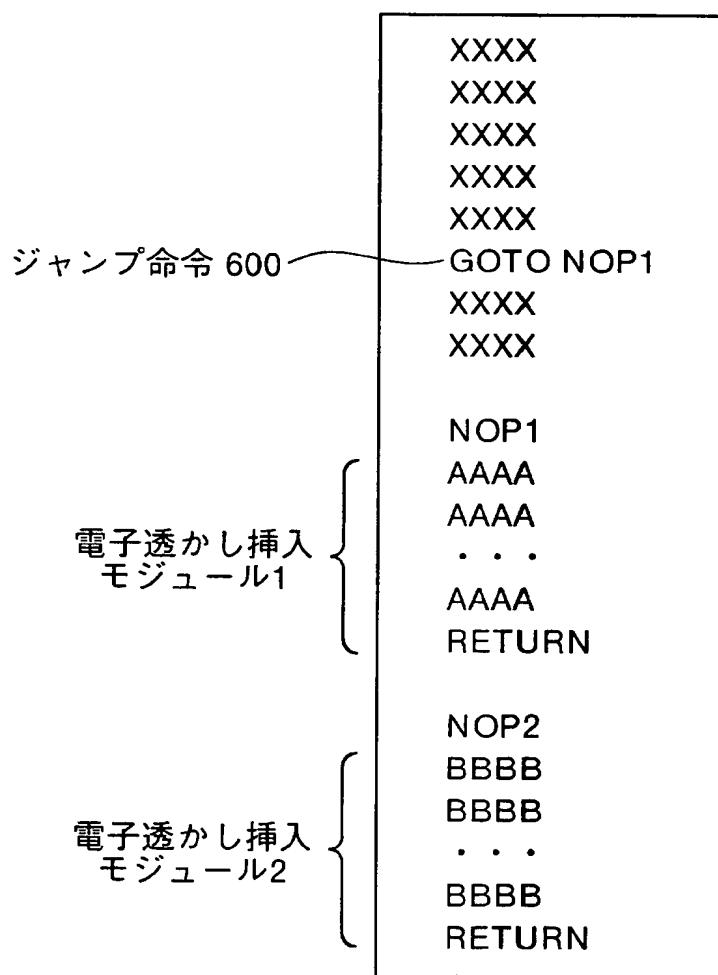
【図 5】

本発明の実施の形態1による画像処理装置における、動画像の再生処理の手順を示すフローチャート



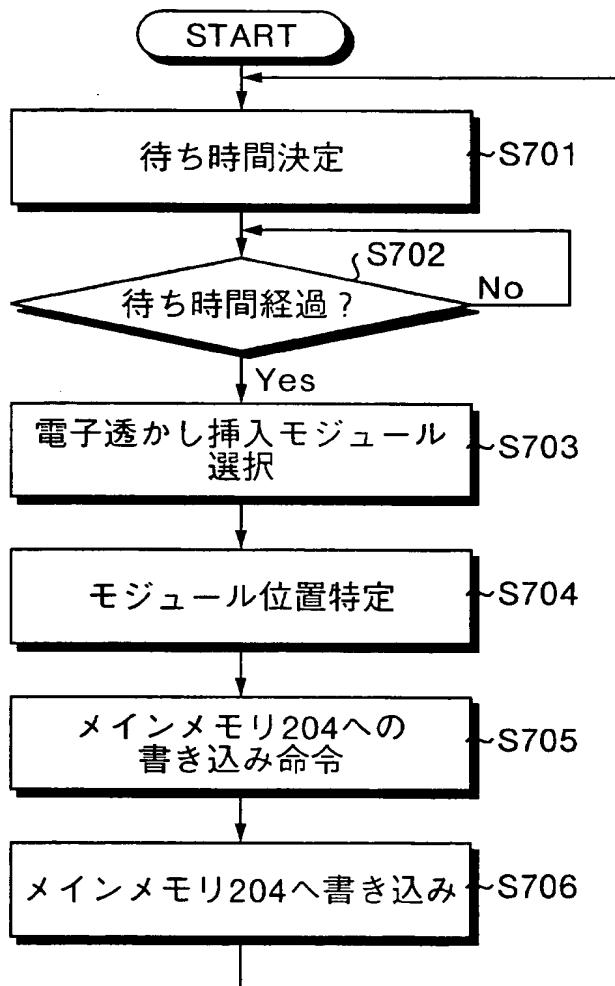
## 【図6】

本発明の実施の形態2による画像処理プログラム作成装置  
(具体的にはTRM208) で作成される、  
画像処理プログラムの内部構造を模式的に示す説明図



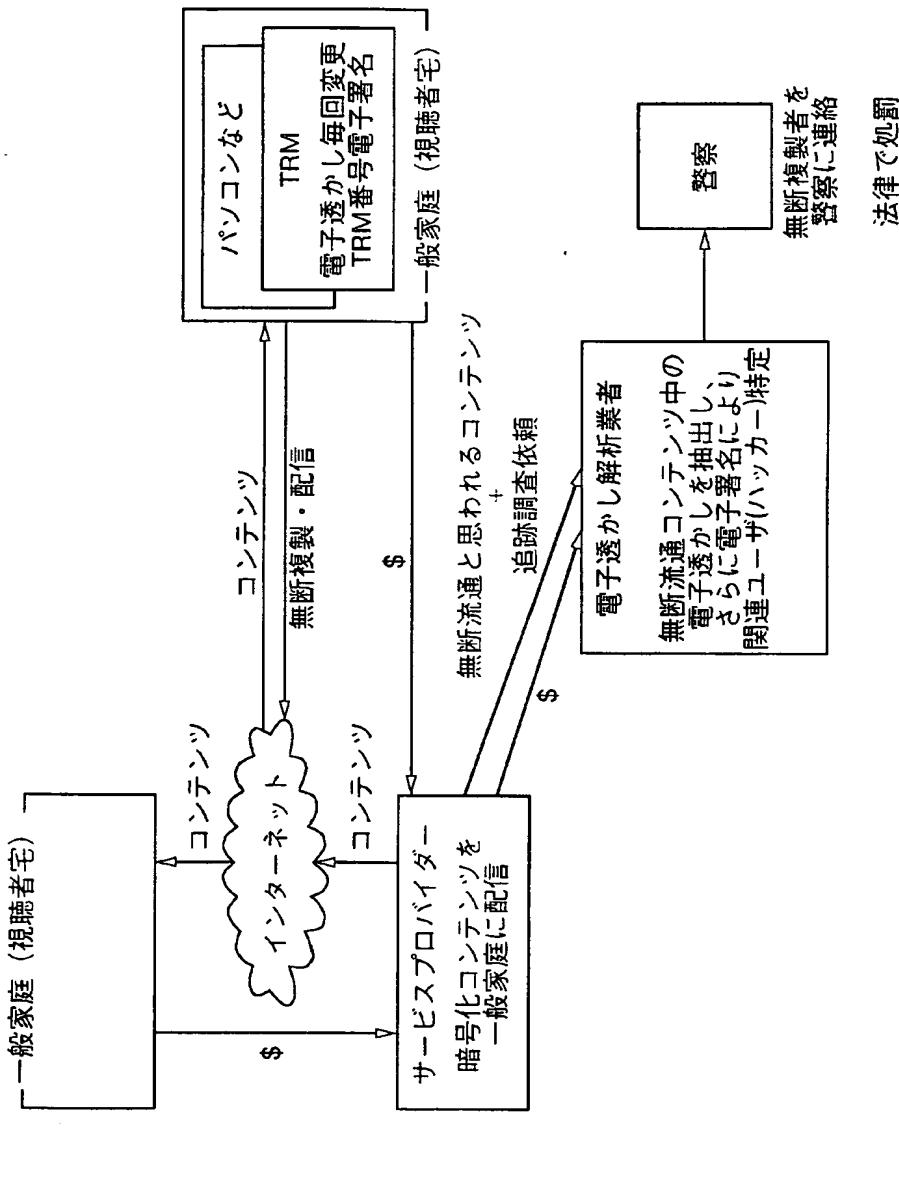
【図7】

本発明の実施の形態2による画像処理プログラム作成装置  
(具体的にはTRM208) における、電子透かし挿入  
モジュール切り替え処理の手順を示すフローチャート



【図 8】

コンテンツが販売されてから違法な複製品の出所が特定されるまでの流れを模式的に示す説明図



【書類名】 要約書

【要約】

【課題】 パソコン内の画像メモリに存在する復号・伸張後の動画像の無断複製や無断配信を抑止すること。

【解決手段】 動画像の提供元があらかじめ埋め込んでいる著作権情報（著作権者など）に加えて、当該動画像の再生時に、その再生元のパソコンに組み込まれているTRM（Tamper Resistant Module）の固有番号を電子透かしとして挿入する。再生の都度、TRMは複数の電子透かし挿入モジュールの中からいずれかをランダムに選択し、選択したモジュールを、MPEG伸張モジュール内の複数のNOP領域のうちランダムに選択した領域に組み込む。再生の都度でなく、一連の動画像の個々の画像ごとにモジュールを切り替えることも可能である。動画像ごと、あるいは画像ごとに透かしの挿入アルゴリズムが異なるので、解析によるその除去（特に全画像からの完全な除去）は非常に困難である。

【選択図】 図4

特願2003-063705

出願人履歴情報

識別番号 [000005223]

1. 変更年月日 1996年 3月26日  
[変更理由] 住所変更  
住 所 神奈川県川崎市中原区上小田中4丁目1番1号  
氏 名 富士通株式会社